

## UNITED STATES DISTRICT COURT

for the  
Eastern District of VirginiaIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)3009 SUMMERSHADE COURT  
HERNDON, VIRGINIA 20171

Case No. 1:22-SW-372

UNDER SEAL

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

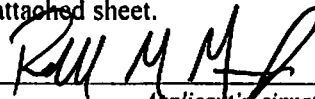
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
21 U.S.C. §§ 841(a)(1) and 846Offense Description  
Conspiracy to Distribute Fentanyl

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.Reviewed by:  
Lauren E. Hahn  
Special Assistant United States Attorney (LT)Applicant's signature  
Task Force Officer Randall M. Mason  
Drug Enforcement Administration

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
\_\_\_\_\_ telephone \_\_\_\_\_ (specify reliable electronic means).Date: 07/06/2022City and state: Alexandria, Virginia

Judge's signature

Hon. Ivan D. Davis, United States Magistrate Judge

Printed name and title

ATTACHMENT A

*Place to be searched*

The premises to be searched is the following, including any and all structures located within the curtilage thereof: 3009 Summershade Court, Herndon, Virginia 20171 (**"TARGET LOCATION"**) is a two-story single-family residence. The sides of the residence are a mixture of gray siding and red brick. The numbers "3009" are affixed horizontally above glass sliding doors on the left side of the residence and vertically on a post that supports the awning to the right of the main front door. The main door to the residence is white in color and is located in the middle of the residence.



**ATTACHMENT B**

*Items to be seized*

The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 21, United States Code, Sections 841 and 846 (Conspiracy to distribute fentanyl) including, but not limited to, the following:

- a. Controlled substances, indicia of distribution, records and documents, receipts, notes, ledgers, and other papers including any computerized or electronic records including cellular telephones, relating to the ordering, purchase or possession of controlled substances;
- b. Items commonly associated with the packaging and sales of controlled substances, including USPS packaging, sealed parcels prepared for mailing, gray and manila bubble mailers, address labels, black foil bags, plastic bags or zip lock bags;
- c. U.S. currency and other illicit gains from the distribution of controlled substances;
- d. Books, records, receipts, notes, ledgers, and other papers including any computerized or electronic records including cellular telephones, relating to the ordering, purchase or possession of controlled substances;
- e. Address and/or telephone books and papers, including computerized or electronic addresses and/or telephone records reflecting names, addresses and/or telephone numbers;
- f. Books, records, receipts, bank statements, and records, money drafts, letters of credit, money order and cashier's checks, receipts, pass books, bank checks, safety deposit box keys and any other items evidencing the obtaining, secreting, transfer, concealment, storage and/or expenditure of money or other assets including, but not limited to, controlled substances;
- g. Firearms, ammunition (including spent ammunition), and indicia of firearm possession, including photos and videos depicting firearm possession, gun cases, gun packaging, gun racks, gun manuals, cleaning kits, tools used for the maintenance of firearms, magazines, ammunition, and packaging for magazines or ammunition;
- h. Documents and papers evidencing ownership of firearms, possession of firearms, storage and location of such assets and facilities to safely store and secure such items, such as safes, to include lock boxes, gun safes, and strong boxes;
- i. Cellular telephones, personal data accessories, computer flash cards, video tapes, compact disks, digital video disks, and other devices and/or electronic media;
- j. Photographs and/or video, in particular photographs and/or videotapes of potential

co-conspirators and their criminal associates, assets, and/or controlled substances, along with personal address lists, and other documents with the names and telephone numbers of potential co-conspirators;

- k. Indicia of occupancy, residence, and/or ownership of the premises described herein, including, but not limited to, utility and telephone bills, cancelled envelopes, and keys;

For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant ("COMPUTER"):

- a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. Evidence of the lack of such malicious software;
- d. Evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. Evidence indicating the COMPUTER user's state of mind as it relates to the crime under investigation;
- f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. Evidence of the times the COMPUTER was used;
- i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- k. Records of or information about Internet Protocol addresses used by the COMPUTER;
- l. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records," "documents," "programs," "applications," "materials," and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the **TARGET LOCATION** described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same

individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

**This warrant authorizes the seizure of any COMPUTER or electronic device. However, with respect to any COMPUTER or electronic device, this warrant authorizes only the search of any COMPUTER or electronic device that is reasonably determined to have been owned or utilized by CHINCHILLA.**

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the DEA may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Any locked container such as a safe may be searched for the property to be seized set forth herein.

If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of government attorneys and agents is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will review all seized communications and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications to/from attorneys. The filter team then will provide all communications that do *not* involve an attorney to the investigative team and the investigative team may resume its review. If the filter team decides that any of the communications to/from attorneys are not actually privileged (*e.g.*, the communication includes a third party or the crime-fraud exception applies), the filter team must obtain a court order before providing these attorney communications to the investigative team.